39. (Unamended) The method of claim 36, further comprising re-directing the data signal to a second resource in response to the credit balance being less than the cost, the second resource configured to allow for increasing the credit balance.

40. (Unamended) The method of claim 36, further comprising providing access to a second resource having no cost in response to the credit balance being less than the cost.

41. (Unamended) The method of claim 36, wherein the cost comprises one from a group comprising a monetary value, a quality of service value, a bandwidth value, a time value, and a content rating value.

42. (Unamended) The method of claim 36, further comprising passing the data signal to a second device having the resource.

REMARKS

Applicants would like to thank the Examiner for the interview on August 13, 2002.

Claims 29-42 are pending in this application. Claims 29 and 36 are amended.

In the Official Action dated May 23, 2002, the Examiner rejected claims 29-32, 35-40 and 42 under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Number 6,272,535 to Iwamura ("Iwamura"). Applicants respectfully traverse these rejections.

Claim 29 now recites:

> A method on a detector device for controlling access to information on a network including a plurality of interconnected devices, the detector device coupled to the network between a first device and a second device such that the detector device does not introduce a point of failure if the detector device becomes inoperable, the method comprising:
>
> monitoring a request signal from the first device for data on the second device in the network, the request signal including a user identification parameter;

determining whether a user identified by the user identification parameter is permitted access to the data; and

comparing a pre-set credit parameter associated with the user with a pre-determined value associated with the data to determine permission to access the data.

The claimed invention controls access to information on a network by determining if a user has permission to access the information and whether the user has sufficient credit to access the information. A detector device monitors a request from a first device for data on a second device and is coupled to the network so that it does not introduce a point of failure into it. The request signal includes a user identification that is used by the detector device to determine if the user can access the information. By monitoring the request signal on the network, the detector device controls access to the information without any special hardware or software in the first device.

Iwamura does not disclose the claimed invention. Iwamura discloses a system in which users request information using terminals or kiosks. Col. 4, lines 8-11. The user terminals send a request for information to the appropriate information provider over the network. Col. 4, lines 11-13. The information providers respond to the requests by sending the information to the user terminal along with a cost associated with the information. Col. 5, lines 11-23. The user terminals include special hardware and/or software for receiving money or credit from the user and determining if the user has input enough money/credit to access the information. Col. 5, line 24 through Col. 6, line 20.

By contrast, the method of claim 29 is performed on a detector device that is "*coupled to the network between a first device and a second device such that the detector device does not introduce a point of failure if the detector device becomes inoperable.*" Iwamura does not disclose a detector device, let alone a detector device coupled to the network such that it does not

introduce a point of failure into the network. Rather, the user terminals disclosed in Iwamura are endpoints of the network and are not coupled between a first device and a second device in a manner as Applicants now claim. Moreover, unlike the claimed invention, if the user terminals disclosed in Iwamura are not functioning the user cannot access the information.

Iwamura also fails to disclose "*monitoring a request signal from the first device for data on the second device in the network, the request signal including a user identification parameter.*" The user terminals disclosed by Iwamura do not monitor request signals and have no need to monitor request signals. Instead, the user terminals send user requests for information to the information provider. Col. 4, lines, 8-13. Thus, the user terminals are more analogous to the first devices in the claimed invention than to a detector device. The user terminals in Iwamura control access to information at the terminals themselves and thus have no need to monitor request signals. However, to control access, the user terminals in Iwamura require special hardware and/or software to receive money/credit from the user and determine if the user has input sufficient money/credit to access the information.

In contrast to Iwamura, the claimed invention does not require any special hardware or software in the device used by the user to request the information because the detector device controls access to the information using the monitored request signal and the user identification parameter. The user identification parameter allows the detector device to "*determine whether a user identified by the user identification parameter is permitted to access the data.*" Iwamura does not disclose this limitation. The user terminals disclosed in Iwamura do not have any knowledge of the user. In fact, one of the objectives listed in the summary of the Iwamura specification is to protect the privacy of the user. Again, the system disclosed in Iwamura has no need to know the user identity since all of the control over the access to information takes place

in the user terminal. Thus, the Iwamura system does not use the user identification to determine whether the user is permitted to access the information.

Hence, in view of the above discussion it is clear that Iwamura does not disclose all of the limitations of claim 29, and therefore, does not anticipate the claimed invention. In addition, claims 30 through 35 are dependent on claim 29 and add additional patentable features of the claimed invention. For example, claim 32 further recites "re-directing the data signal to a third device in response to the pre-set credit parameter being less than a predetermined value, the third device allowing for a re-setting of the pre-set credit parameter to a new pre-set credit value comprising a value greater than or equal to the predetermined value." This claimed feature is also not disclosed by Iwamura. Nor does Iwamura disclose each claimed feature of claim 33, as Examiner correctly notes in the Official Action. Again, Applicants respectfully submit that Iwamura fails to disclose the invention of these claims and claim 30, 31, 34, and 35.

Similar to claim 29, claim 36 also contains the limitations that are not disclosed by Iwamura. The arguments set forth above with respect to claim 29, and its dependent claims 30-35, are also applicable to claim 36 and its respective dependent claims 37-42, and those arguments are herein incorporated by reference.

Claims 33-34 and 41 were rejected under 35 U.S.C. 103(a) as being unpatentable over Iwamura in view of "Some FAQs about Usage-Based Pricing" (herein "Pricing"). Claims 33 and 34 are dependent on claim 29 and claim 41 is dependent on claim 36. As discussed above, Iwamura does not disclose all of the limitations of claims 29 and 36. With regard to the Pricing reference, Applicants respectfully submit that this reference does not provide a teaching or suggestion to combine this reference with Iwamura in a manner as is now claimed by Applicants.

Therefore, Applicants submit that claims 33, 34 and 41 are patentably distinguishable over the combination of Iwamura and Pricing.

In sum, Applicants respectfully submit that claims 29-42, as presented herein, are patentably distinguishable over the cited references (including references cited but not applied). Therefore, Applicants now request reconsideration and allowance of these claims.

In addition, Applicants respectfully invite Examiner to contact Applicants' representative at the number provided below if Examiner believes it will help expedite further prosecution of this application.

Respectfully submitted,
STANISLAV KHIRMAN,
MARK RONALD STONE,
OREN ARIAL,
ORI COHEN

Dated: August 23, 2002

By: _____

Rajiv P. Patel, Reg. No. 39,327
Fenwick & West LLP
Two Palo Alto Square
Palo Alto, CA 94306
Telephone: (650) 858-7607
Facsimile: (650) 494-1417

Attachment: Claim Revisions

VERSION WITH MARKINGS TO SHOW CHANGES MADE

29. A method on a detector device for [of] controlling access to information [from a device] on a network including a plurality of interconnected devices, the detector device coupled to the network between a first device and a second device such that the detector device does not introduce a point of failure if the detector device becomes inoperable, the method comprising:

monitoring a request signal from [a] the first device for data on [a] the second device in the network, the request signal including a user identification parameter;

[determining whether the access to the data requires a credit value;]

determining whether a user identified by the user identification parameter is permitted access to the data; and

[detecting a pre-set credit parameter in the request signal; and]

comparing [the]a pre-set credit parameter associated with the user with a pre-determined value associated with the data to determine permission to access the data.

36. A network-based billing method on a detector device for providing access to resources on a network, the detector device coupled to the network such that the detector device does not introduce a point of failure if the detector device becomes inoperable, the method comprising:

monitoring a data signal from a device on a network, the data signal including a request for a resource[, the resource including a value parameter];

identifying a cost for accessing the resource;

associating a user identification with the data signal;

determining whether a user identified by the user identification is permitted access to the resource;

identifying a credit balance for the user identification; and

comparing the credit balance with the cost to determine access to the resource.[; and]